VMware vDefend Firewall
Specific Program Documentation ("SPD")

The Broadcom software program(s) ("Broadcom Software" or "Software") listed below is provided under the following terms and conditions in addition to any terms and conditions referenced on the Broadcom quote, order form, statement of work, or other mutually agreed ordering document (each a "Transaction Document") under the applicable end user agreement or governing contract (collectively, the "Agreement") entered into by Customer and the Broadcom entity ("Broadcom") through which Customer obtained a license for the Broadcom Software. These terms shall be effective from the effective date of such Transaction Document. Capitalized terms have the meanings ascribed to them herein, or, otherwise, in the Agreement (including the VMware Licensing Glossary).

Program Name: ***ALL VMWARE PRODUCTS LISTED IN THE TABLE BELOW***

1. DEFINITIONS.

All terms defined in the VMware Licensing Glossary located at https://www.broadcom.com/company/legal/licensing apply to this SPD unless specified herein.

"**Authorized Users**" means Customer, its employees and independent contractors and/or Customer Affiliates that access and use Software provided that they are bound by terms and conditions no less restrictive than those contained in the Agreement and solely to the extent that they are acting on behalf of Customer or Customer Affiliates.

"**Container Security with Antrea**" means an environment where Antrea is deployed in a container cluster.

"Distributed Firewall" means an environment where VMware vDefend Distributed Firewall is enabled to cover a virtualized host.

"**DPU**" is a data processing unit. This means a single, physical chip that houses at least one Physical Core that can execute computer programs and is incorporated into a SmartNIC.

"**Gateway Firewall"** – means an environment where the VMware vDefend Gateway Firewall is enabled either on a virtual or Bare Metal environment.

"SmartNIC" is a hardware component that converts data packages to signals spread throughout a network. It is a programmable extension of an interface card (NIC).

"**Software Gateway Instance"** is a virtual network function that delivers network services and provides optimized data paths to applications, network branches and data centers.

"**Tool Box**" means certain software tools that VMware may provide to Customer from time to time for support purposes.

"**VMware vDefend Firewall as a Bare Metal Agent**" means an environment where an agent covers a bare metal host.

"**VMware vDefend Firewall on DPU**" means a customer is running VMware vDefend Firewall as a Distributed Firewall or Gateway Firewall AND those features are offloaded onto the DPU of a host.

2. USE RIGHTS AND LIMITATIONS.

There are three editions of the VMware Firewall available for license: VMware vDefend Firewall, VMware vDefend Firewall with Advanced Threat Prevention (ATP), and VMware vDefend Advanced Threat Prevention Add-on.

Each edition of VMware Firewall includes entitlements to use different functionality and inclusions. For the edition of the Broadcom Software Customer has purchased licenses for, Customer may only use the functionality for that edition as specified at https://knowledge.broadcom.com/external/article?legacyId=89137.

If the Transaction Document indicates that Customer has received a license for any of the below Broadcom Software, Customer use of such Broadcom Software is subject to the applicable following limitations:

Broadcom Software	License Use, Meter, and Model; Additional Limitation(s) for Broadcom Software
VMware vDefend Firewall	Customer may use the Broadcom Software for applicable number of Cores as outlined on the section Deployment Specific Purchase Requirements.
VMware vDefend Firewall with Advanced Threat Prevention (ATP)*	Customer may use the Broadcom Software for applicable number of Cores as outlined on the section Deployment Specific Purchase Requirements. Customer license includes a Cloud Service feature for user interface and analysis and storage of network traffic and artifacts for the same duration as Customer's Subscription term.
VMware vDefend Advanced Threat Prevention Add-on *	Customer may use the Broadcom Software for applicable number of Cores as outlined on the section Deployment Specific Purchase Requirements. Customer license includes a Cloud Service for user interface and analysis and storage of network traffic and artifacts for the same duration as Customer's Subscription term.

** VMware vDefend Firewall with Advanced Threat Prevention and VMware vDefend Advanced Threat Prevention Add-on editions of this Software include optional cloud-based features. This SPD governs Customer's use of the Software. Customer's use of optional cloud-based features is subject to the terms of the VMware vDefend Firewall SaaS Listing (i.e. not this SPD).*

The Software is licensed as Subscription Software. Customer may use the Software and Support solely during the Subscription term. Customer must pay for all the Software Customer uses.

At the end of the Subscription term, Customer may have the option to renew the Subscription licenses. If Customer does not renew, the Subscription licenses shall expire at the end of the Subscription term. Upon expiration or termination of Customer's licenses to the Software, Customer must cease use of the Software, Documentation and Support and certify cessation of use to VMware. VMware may, at its discretion, retire Software and/or Support from time to time.

Deployment Specific Purchase Requirements. Customer will have entitlement to the license of the Broadcom Software referenced in Customer's Transaction Document. If multiple types of deployment are shared on the same host, each deployment will independently require the appropriate number of licenses. Each edition of VMware vDefend Firewall can be deployed in the following types of deployment.

- When deploying VMware Firewall as a Distributed Firewall, Customer must purchase one (1) Core of VMware Firewall to deploy one (1) Core of Distributed Firewall.
- When deploying VMware Firewall as a Gateway Firewall, Customer must purchase four (4) Cores of VMware Firewall to deploy one (1) Core of Gateway Firewall.
- When deploying VMware Firewall for Container Security with Antrea, Customer must purchase one (1) Core of VMware Firewall to deploy one (1) Core of Container Security with Antrea.
- When deploying VMware Firewall as an agent for Bare Metal workloads, Customer must purchase one (1) Core of VMware Firewall for every four (4) Cores of Bare Metal.
- When deploying VMware Firewall on a DPU, in addition to the entitlement required to deploy as a Distributed Firewall or Gateway Firewall, the Customer must purchase four (4) Cores of VMware Firewall to secure one (1) DPU.
- When deploying VMware Firewall to monitor of Desktop environments as outlined by VMware Firewall for Desktop,

Customer may deploy 2.5 Concurrent Users for every (1) Core of VMware Firewall Customer purchases.

VMware Firewall for Desktop. Customer may use the Broadcom Software for up to the number of Concurrent Users or Authorized Users for which Customer has paid the applicable license fees when only used in Clusters running (i) virtual desktop virtual machines, including those desktops from VMware Horizon and/or third party solutions, (ii) a Terminal Services Session or remote desktop services host for the purpose of hosting session based desktops or remoting applications, and (iii) associated desktop management and monitoring tools. For each Cluster that is running the Broadcom Software, Customer must purchase a license for every Concurrent User or Authorized User using the Broadcom Software in the Cluster.

Customer may use the Broadcom Software to monitor up to the number of Cores for which Customer has paid the applicable license fees. The Broadcom Software is licensed as Subscription Software. Customer may use the Broadcom Software solely during the Subscription Term. Upon expiration or termination of Customer's licenses to the Subscription Software, Customer must promptly cease use of the Broadcom Software and Documentation.

APIs and Third Party Applications. Customer may use the APIs included with the Broadcom Software only to integrate the Broadcom Software with Customer's cloud management, network management and billing systems. Any use of the APIs or other portions of the Broadcom Software for other services (including but not limited to protocols, traffic engineering, L4-L7) must be certified for use in writing by VMware and will be subject to Customer's payment of additional fees. Customer may not use the Broadcom Software, including the APIs, with any third party applications written specifically for the Broadcom Software unless otherwise authorized in writing by VMware, which authorization may be conditioned on the payment of additional fees to VMware for such use.

Threat Intelligence Data Collection. Certain Software offerings may collect data relating to malicious or potentially malicious code, attacks, and activities on Customer's network ("**Threat Intelligence Data**"). Threat Intelligence Data is collected by VMware for analysis and possible inclusion in a threat intelligence feed utilized by certain VMware vDefend Firewall offerings. Prior to inclusion in any threat intelligence feed, Threat Intelligence Data will be: (i) reduced to a unique file hash or to queries or general behavioral descriptions that can be used to identify the same or similar malicious or potentially malicious code in Customer's and other customers' systems; and/or (ii) anonymized and made un-attributable to any customer or individual. VMware may distribute Threat Intelligence Data at its discretion as part of its threat intelligence data feed or in published reports or research. By using a Threat Intelligence Data feed, Customer is deemed to have agreed that Threat Intelligence Data is not Customer Data, and VMware may retain, use, copy, modify, distribute, and display the Threat Intelligence Data for its business purposes, including without limitation for developing, enhancing, and supporting products and services, and for use in its threat intelligence feed or in published reports or research. The information provided via any threat intelligence feed is provided on an "AS-IS" and "AS-AVAILABLE" basis only.

VMware Security Intelligence Data. VMware Security Intelligence collects data relating to traffic flows, activities on Customer's network, and VMware system configuration and state ("**VMware Security Intelligence Data**"). VMware may use VMware Security Intelligence Data for analysis, verification, and enhancement of our products, including but not limited to enhancements to visualization, automated suggestions, and recommendation of network security policies and related configurations of VMware offerings for Customer and for other customers. VMware Security Intelligence Data will be: (i) transformed to mask any information or general behavioral descriptions that can be used to identify any of Customer's systems or other customers' systems; or (ii) anonymized and made un-attributable to any customer or individual. VMware may distribute VMware Security Intelligence Data at its discretion as part of other products or in published reports or research. By using VMware Security Intelligence, Customer agrees that VMware Security Intelligence Data is not Customer Data. The recommendations and suggestion provided by VMware Security Intelligence are provided on an "AS-IS" and "AS-AVAILABLE" basis only without any indemnification, support, or warranty of any kind, express or implied.

Tool Box. Customer may internally use the Tool Box only to obtain support from VMware pursuant to the Services Terms. The Tool Box shall be deemed "Broadcom Software" for the purposes of the Agreement.

3. THIRD PARTY INFORMATION AND TERMS.

Any required third-party software license terms are incorporated by this reference and are set forth in online documentation at techdocs.broadcom.com or legaldocs.broadcom.com.


BROADCOM®